

# **EXHIBIT 1**

**FILED UNDER SEAL**

**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
	)	
v.	)	<b>Criminal No. 1:20-cr-143</b>
	)	<b>UNDER SEAL</b>
<b>ZACKARY ELLIS SANDERS,</b>	)	
<b>Defendant.</b>	)	

**SEALED MEMORANDUM OPINION**

On February 10, 2020, Federal Bureau of Investigation Special Agent Christopher Ford applied for a search warrant for defendant Zackary Ellis Sanders's residence. In connection with the warrant application, Special Agent Ford prepared a search warrant affidavit. On February 10, 2020, Magistrate Judge John F. Anderson authorized a search warrant for the residence, and, on February 12, 2020, the FBI executed the search warrant. On June 24, 2020, a federal grand jury returned a twelve-count indictment charging defendant with five counts of production of child pornography in violation of 18 U.S.C. § 2251(a) and § 2251(e), six counts of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and § 2252(b)(1), and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and § 2252(b)(2).

At issue now in this matter is defendant's Motion to Compel Discovery. Defendant argues that under Rule 16, Fed. R. Crim. P., *Brady v. Maryland*, and the Sixth Amendment, defendant is entitled to additional discovery in two areas:

(1) Whether the government had actual evidence that the Internet user with the Internet Protocol ("IP") address 98.169.118.39, which allegedly belongs to defendant, "accessed online child sexual abuse and exploitation material via a website." Search Warrant Affidavit at ¶ 23.

(2) Whether Special Agent Ford knew that a Foreign Law Enforcement Agency (FLA) referred to in the search warrant affidavit had used an investigative method to interfere with, access, search, and/or seize data from a computer in the United States to generate its

tip to the FBI regarding IP address 98.169.118.39. *See* Search Warrant Affidavit at ¶ 25.

Defendant has indicated that he plans to file a pretrial motion attacking the search warrant's validity based on alleged misrepresentations in ¶¶ 23 and 25 of the search warrant affidavit.<sup>1</sup>

This matter has been fully briefed, orally argued, and is now ripe for disposition. For the reasons that follow, defendant's Motion to Compel must be denied in its entirety; defendant's discovery request does not satisfy the threshold requirement for materiality under Rule 16, Fed. R. Crim. P., and neither *Brady v. Maryland* nor the Sixth Amendment right to counsel supports defendant's Motion to Compel.

### I.

The following information relevant to defendant's Motion to Compel is derived from the exhibits attached to the defendant's Motion to Compel Discovery, the government's opposition brief, the defendant's reply brief, and the parties' supplemental submissions.<sup>2</sup> Essential to an understanding of defendant's Motion to Compel are the following general summary of the Tor internet network and discussion of the investigation of defendant.

- An Internet Service Provider offers subscribing internet users access to the internet and

---

<sup>1</sup> Specifically, defendant indicates in his briefing that he intends to file a motion to suppress and seek a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Under *Franks*, a defendant seeking to challenge a search warrant affidavit must first make a substantial preliminary showing to obtain a hearing:

[W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

*Id.* at 155–56. If a defendant then makes the requisite showing at a *Franks* hearing, the fruits of the challenged search warrant must be excluded. *See id.* at 156.

<sup>2</sup> After defendant's Motion to Compel was fully briefed and oral argument was held, the parties were afforded an additional ten days from the date of oral argument, or until August 10, 2020, to submit any additional matter they wished to have considered prior to the motion's disposition. Following submission of these supplemental briefs, defendant sought and obtained leave to file a response to the government's supplemental brief, and the government was afforded an opportunity to reply to defendant's response on or before Wednesday, August 19, 2020.

gives each internet user an Internet Protocol (IP) address.

- When a typical internet user visits a website using a browser such as Safari, the internet user provides his IP address information to the website, and that IP address information is visible in the website's IP address log. This exchange of IP address information permits the website to deliver requested information to the internet user.
- Some internet users attempt to use the internet anonymously through services such as the Tor network, which is accessible if an internet user downloads special software such as the Tor Browser.
- The Tor network routes Tor user communications or information requests through several relay computers, called "nodes," along a randomly assigned path called a "circuit." The Tor network is composed of thousands of nodes operated by individuals or entities who have donated computers or computing power to facilitate the Tor network's operation.
- Each node can view the address information of the node that sent the information request and the address information for the next node where the information request should be sent. But the content of the internet user's information request is encrypted as the request travels through a node.
- For a Tor user, a destination website's IP address log will only show that the IP address of the last node in a given circuit sent an information request to the destination website. These features of Tor hinder law enforcement officers' efforts to determine the true IP addresses of Tor users.
- A Tor user can access certain "hidden services" or "onion services" websites that are not accessible to non-Tor internet users. These hidden services websites operate in a manner designed to obscure the true IP address of the computer hosting the website. There are no publicly available listings for determining the IP address of a computer server hosting a Tor hidden services website. These features of Tor hidden services websites hinder law enforcement officers' efforts to determine the true IP address of a computer hosting a Tor hidden services website.
- A Network Investigative Technique offers one method for de-anonymizing Tor users. A Network Investigative Technique is a process that interferes with the Tor Browser's security protections and forces a Tor user's computer to create a non-Tor connection with the computer used to deploy the Network Investigative Technique. This non-Tor connection allows for identification of the Tor user's true IP address. This process involves interference with the Tor user's computer.
- On August 19, 2019, [REDACTED] wrote an [REDACTED] on [REDACTED] stating that

On 2019-05-23 02:06:48 UTC [IP Address] 98.169.118.39 was used to access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [REDACTED]

Users were required to create an account (username and password) in order to access the majority of the material.

August 19, 2019 [REDACTED] Report.

- In August 2019, the FBI received a tip from [REDACTED] the FLA, based on the [REDACTED] report.
- On September 16, 2019, [REDACTED] sent a letter to a Supervisory Special Agent at the FBI stating that [REDACTED] had provided the FBI with “data . . . in relation to Internet addresses (IPs), associated to individuals who have accessed online Child Sexual Abuse and Exploitation material.” September 16, 2019 [REDACTED] Letter. The September 16, 2019 letter stated that the IP address data was “obtained [REDACTED] [REDACTED]” based on two warrants [REDACTED] [REDACTED]. *Id.* The [REDACTED] Letter states that “at no time was any computer or device interfered with in the United States” and that “[u]nder these warrants during an independent investigation lawfully authorized under [REDACTED] legislation, [REDACTED] did not access, search or seize any data from any computer in the United States.” *Id.*
- The [REDACTED] created an [REDACTED] Report for an operation, [REDACTED] entitled “CSAE Imagery on Tor Hidden Service Site [REDACTED].” October 25, 2019 [REDACTED] Report. The [REDACTED] Report identifies five images or videos shared on “the TOR Hidden Service [REDACTED]” and states that “[t]his site had an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [REDACTED] [REDACTED]. Users were required to create an account (username and password) in order to access the majority of the material.” *Id.* On October 25, 2019, the [REDACTED] sent the [REDACTED] Report to “International partners in receipt of [REDACTED],” including the FBI. *Id.*<sup>3</sup> The October 25, 2019 [REDACTED] Report does not state that IP address 98.169.118.39 created or accessed the five images or videos identified in the Report.
- On January 17, 2020, Special Agent Christopher Ford wrote a report to open an investigation into IP address 98.169.118.39. January 17, 2020 FD-1057. Special Agent Ford’s report describes a website [REDACTED] as “an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately 2016 to June 2019.” *Id.* at 1.
- Special Agent Ford’s FD-1057 stated that “[i]n August 2019, the FBI received information from a foreign law enforcement agency (FLA) known to the FBI with a history of providing reliable, accurate information in the past that [the] FLA identified a user who accessed [REDACTED] using IP address 98.169.118.39, on May 23, 2019, at

<sup>3</sup> The government represents that the date this document was sent [REDACTED] to the FBI was October 25, 2019. The document itself lists the “Time/Date of Report” as “27/07/2020 15:59,” but counsel for the government explains that this document’s listed date was the product of an automatic update performed by Microsoft Word, not a reflection of the date the document was actually transmitted.

02:06:48 UTC.” *Id.* at 2.

- Special Agent Ford’s FD-1057 states that an administrative subpoena was issued on September 10, 2019 to Cox Communications for information related to IP address 98.169.118.39 on May 23, 2019, at 02:06:48 UTC. January 17, 2020 FD-1057 at 2. Pursuant to the subpoena, Cox Communications identified the subscriber as Risa Sanders [REDACTED], McLean, VA 22102-1452. *Id.* The FD-1057 also states that Risa Sanders is a licensed clinical psychologist. *Id.* at 3.
- Special Agent Ford’s FD-1057 reflects that the FBI obtained information about the other residents at the [REDACTED], McLean, VA 22102-1452 address, Jay H. Sanders and Zackary E. Sanders. January 17, 2019 FD-1057 at 3.
- The FD-1057 concluded that “[b]ased on the provided information, the user of the IP address 98.169.118.39 is in violation of 18 U.S.C. 2252(a)(2) Sexual Exploitation of Children, specifically distribution of child pornography.” January 17, 2020 FD-1057 at 4.
- On February 10, 2020, Special Agent Ford applied for a search warrant and submitted an affidavit in support of the application. In the affidavit, Special Agent Ford averred:

A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the “TARGET WEBSITE.” There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

Affidavit ¶ 6.

- Special Agent Ford also averred that because the Tor network makes it more difficult for law enforcement agencies to determine where a hidden services website or Tor users who access that website are located, a law enforcement agency in one country may share information with a law enforcement agency in another country where a hidden services website is located or where a Tor user appears to reside. *See* Affidavit ¶ 22.
- Special Agent Ford also averred that:

In August 2019, a foreign law enforcement agency (“FLA”) known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that the FLA determined that on May 23, 2019, a user of the IP address 98.169.118.39 accessed online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

Affidavit ¶ 23.

- Special Agent Ford further averred:

The FLA described the website as having “an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [REDACTED],” stated that “[u]sers were required to create an account (username and password) in order to access the majority of the material,” and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

Affidavit ¶ 24.

- Special Agent Ford also averred that:

The FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with the FLA and the FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. The FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in the FLA’s country pursuant to its national laws. The FLA further advised U.S. law enforcement that the FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which the FLA identified the IP address information provided by the FLA.

Affidavit ¶ 25.

- On February 10, 2020, Magistrate Judge John F. Anderson authorized the Search Warrant for defendant’s residence. Two days later, on February 12, 2020, law enforcement agents executed the Search Warrant.
- Defendant was arrested and made an initial appearance on March 20, 2020. The government moved for defendant’s detention. During the litigation regarding defendant’s detention, the government represented that “[t]he defendant came to the government’s attention after an investigation conducted by the Federal Bureau of Investigation [ ] and other law enforcement entities revealed that an individual accessed a website that advertises child pornography using an IP address associated with the defendant’s residence in McLean, Virginia.” Government’s Opposition to Revocation of Detention Order at 2.
- After the parties agreed to a protective order related to discovery on April 27, 2020, the government produced the search warrant affidavit to defendant. Since reviewing the search warrant affidavit, defendant has made several discovery requests to the government.



## II.

Defendant argues that Rule 16, Fed. R. Crim. P., *Brady v. Maryland*, and the Sixth Amendment right to effective assistance of counsel require the government to disclose the materials sought by defendant.

Defendant primarily relies on Rule 16, Fed. R. Crim. P., as a basis for obtaining the materials sought by defendant. Under Rule 16(a)(1)(E):

Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

- (i) the item is material to preparing the defense;
- (ii) the government intends to use the item in its case-in-chief at trial; or
- (iii) the item was obtained from or belongs to the defendant.

Fed. R. Crim. P. 16(a)(1)(E). It is clear that defendant has made a discovery request and that this request seeks items that defendant asserts are “within the government’s possession, custody, or control.” Fed. R. Crim. P. 16(a)(1)(E). The parties’ dispute thus focuses on whether defendant’s request seeks items that are “material to preparing the defense.” Fed. R. Crim. P. 16(a)(1)(E).

For a defendant to show materiality under Rule 16(a)(1)(E), Fed. R. Crim. P., “[t]here must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor.” *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010) (quoting *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975)). The requirement that evidence be “material” is satisfied “as long as there is a strong indication that [the material requested] will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.” *Caro*, 597 F.3d at 621 (quoting *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993)).



Evidence that would alter the quantum of proof in a defendant's favor with respect to a *Franks* motion or a suppression motion satisfies Rule 16's materiality standard.<sup>4</sup> This is so because a successful *Franks* motion or suppression motion would affect the government's ability to present evidence in its case-in-chief and thus the government's ability to prove defendant's guilt. *See Caro*, 597 F.3d at 621 (4th Cir. 2010) (requiring showing that requested evidence would allow defendant "significantly to alter the quantum of proof in his favor") (quoting *Ross*, 511 F.2d at 763).<sup>5</sup>

But importantly, to satisfy the materiality requirement, a defendant "must present facts which would tend to show that the Government is in possession of information helpful to the defense." *Caro*, 597 F.3d at 621 (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)). In this respect, courts have held that "[n]either a general description of the information sought nor conclusory allegations of materiality suffice." *Id.* To authorize discovery based on a defendant's mere speculation that the government possesses information that would be helpful to the defense would permit an impermissible fishing expedition. *See United States v. Maranzino*, 860 F.2d 981, 985 (10th Cir. 1988) ("Rule 16 does not authorize a blanket request to see the prosecution's file."). Here, defendant's Motion to Compel fails because he does not satisfy the

---

<sup>4</sup> *See United States v. Cranson*, 453 F.2d 123, 126 n. 6 (4th Cir. 1971) (noting that Rule 16 provided an avenue for a defendant "to secure pre-trial information on identification procedures undertaken by the government in advance of trial as a basis for a motion to suppress"); *see also United States v. Wilford*, 961 F. Supp. 2d 740, 756 (D. Md. 2013) (citing *Cranson* and reasoning that information material to motion to suppress would satisfy Rule 16's materiality requirement).

Out-of-circuit authority also supports this understanding of Rule 16's materiality requirement. *See United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003) (holding that Rule 16 requires disclosure of information about drug-sniffing dog sought to pursue a motion to suppress); *United States v. Mitrovich*, — F. Supp. 3d —, 18-CR-789, 2020 WL 2084991, at \*3–5 (N.D. Ill. April 30, 2020) (requiring disclosure where defendant made *prima facie* showing that requested items were material to motion to suppress).

<sup>5</sup> Indeed, as counsel for the government acknowledged at oral argument, assuming *arguendo* that defendant prevailed on a motion to suppress, the suppression of evidence would present problems for the government's case-in-chief.

materiality requirement; defendant merely speculates that the government possesses additional information that would show that paragraphs 23 and 25 of the search warrant affidavit are inaccurate. This speculation is insufficient to support a motion to compel under Rule 16, Fed. R. Crim. P.

Specifically, defendant contends that the evidence demonstrates that defendant is entitled to additional discovery in two areas. First, defendant argues that the FLA's August 19, 2019 tip, Special Agent Ford's January 17, 2020 FD-1057, paragraph 23 of the February 10, 2020 search warrant affidavit, and the government's March 20, 2020 filing use different language that, in defendant's view, shows that the search warrant affidavit included an intentional misrepresentation, namely that defendant accessed child sexual abuse and exploitation material, when, in defendant's view, the evidence only showed that defendant visited the homepage of a website containing both legal and illegal content. To bolster this argument, defendant seeks discovery regarding the government's contemporaneous understanding of what internet content the internet user did and did not access.

Defendant has not made the requisite showing of materiality necessary to obtain additional discovery regarding paragraph 23 of the search warrant affidavit. Specifically, defendant has not "present[ed] facts which would tend to show that the Government is in possession of information helpful to the defense." *Caro*, 597 F.3d at 621 (quoting *Mandel*, 914 F.2d at 1219). Defendant's argument falters because defendant has not shown that any misrepresentation has occurred here. Paragraph 23 conveys the same information contained in the FLA's tip, namely that on May 23, 2019, a user of the IP address 98.169.118.39 accessed online child sexual abuse and exploitation material via a website.

A comparison of the two statements shows no meaningful difference between the FLA's

tip and the search warrant affidavit's language. The August 19, 2019 [REDACTED] Report states:

On 2019-05-23 02:06:48 UTC [IP Address] 98.169.118.39 was used to access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [REDACTED]. Users were required to create an account (username and password) in order to access the majority of the material.

August 19, 2019 [REDACTED] Report. The February 10, 2020 search warrant affidavit states:

23. In August 2019, a foreign law enforcement agency ("FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that the FLA determined that on May 23, 2019, a user of the IP address 98.169.118.39 accessed online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

24. The FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [REDACTED]," stated that "[u]sers were required to create an account (username and password) in order to access the majority of the material," and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

Search Warrant Affidavit ¶¶ 23–24. The search warrant affidavit clearly communicates the same information contained in the FLA's tip, and defendant's argument to the contrary fails to persuade.

Seeking to avoid this result, defendant argues that "via a website" appears nowhere in the FLA's tip. This argument is unpersuasive; stating that material was accessed "via a website" adds no information because it is obvious that the FLA's original tip describes an internet user's activity on a website. The descriptions in Special Agent Ford's FD-1057 and the government's March 20, 2020 filing do not alter this conclusion. *See* January 17, 2020 FD-1057 (stating that the "FLA identified a user who accessed [REDACTED] using IP address 98.169.118.39, on May 23, 2019, at 02:06:48 UTC"); Government's Opposition to Revocation of Detention Order at 2

(asserting that evidence showed that an individual “accessed a website that advertises child pornography using an IP address associated with the defendant’s residence in McLean, Virginia”). This is so because an internet user cannot access child sexual abuse and exploitation material without accessing a website that advertises and distributes child pornography. There is no evidence—either in documents generated by the FLA or by the FBI—that Special Agent Ford thought defendant merely visited [REDACTED] homepage and did not view child sexual abuse and exploitation material. Defendant’s contrary theory does not satisfy defendant’s burden of setting forth facts to show that the government possesses additional information helpful to the defense. In sum, defendant’s repeated incantation that the government misrepresented the FLA’s tip does not make it so where, as here, every description of the FLA’s tip is consistent.

Second, with respect to paragraph 25, defendant argues that regardless of what assurances the FLA provided to the FBI about the technique used to obtain the tip information, the FBI agent should have known that the FLA interfered with a computer in the United States to identify IP address 98.169.118.39 as an internet user who accessed child sexual abuse and exploitation material via the website [REDACTED]. In other words, defendant contends that the FBI relied on the FLA’s implausible statements to obtain a search warrant. In support of this argument, defendant relies on (i) declarations from a computer expert, Dr. Matthew Miller,<sup>6</sup> (ii) a declaration from an expert [REDACTED],<sup>7</sup> and (iii) statements from FBI agents in previous cases

---

<sup>6</sup> Dr. Miller asserts that “in this case, the [FLA] most likely had to interfere with the Tor Browser’s security protections to take control of, access, interfere with and/or search the contents of computers that visited the target Tor Onion Service website to determine the true IP addresses of those Internet users.” July 12, 2020 Declaration of Dr. Matthew Miller, at 5, ¶ 19.

<sup>7</sup> Defendant’s expert [REDACTED], posits that these warrants [REDACTED] Declaration of [REDACTED] at 2, ¶ 7.



describing Network Investigative Techniques as necessary to identify internet users accessing hidden services websites.<sup>8</sup> To support his theory that the FBI knew that the FLA's tip was false, defendant seeks discovery regarding the government's contemporaneous understanding of the FLA's investigative technique used to generate the tip.

This allegation of implausibility is unpersuasive and fails to provide a basis for authorizing further discovery in this case. As the government correctly notes, the search warrant affidavit communicates the same information contained in the FLA's tip. The defendant thus provides no basis for questioning the veracity of Special Agent Ford's search warrant affidavit. Defendant's speculation that the FLA must have used a technique previously used by the FBI or must have used the technique identified by defendant's expert fails to present facts that show that the government possesses additional information that would be helpful to the defense. Indeed, the government has provided a sworn affidavit from Special Agent Ford identifying alternative, publicly known methods of de-anonymizing Tor users without interfering with a Tor user's computer. *See* August 10, 2020 Declaration of Special Agent Christopher A. Ford. Defendant's theory that the FLA most likely used a Network Investigative Technique does not satisfy Rule 16's requirement that the defendant "present facts which would tend to show that the Government is in possession of information helpful to the defense." *Caro*, 597 F.3d at 621 (quoting *Mandel*, 914 F.2d at 1219).

Also meritless is defendant's suggestion that the United States prompted ██████ to use investigative methods not authorized under United States law before feigning ignorance about

---

<sup>8</sup> For example, defendant argues that prior cases in the Eastern District of Virginia have involved search warrant affidavits stating that a network investigative technique was the only method that the affiants in those cases knew of to identify the IP address of an internet user where, as here, the target website was a Tor Onion Service website. *See United States v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016).

those methods. *See* Defendant's Motion to Compel at 14 ("[T]he US, in effect, outsourced [REDACTED] [REDACTED] investigative processes that would be illegal under US law and then feigned ignorance of that process in seeking its warrant."). Defendant's suggestion is pure hopeful speculation; simply because the FBI and the [REDACTED] FLA communicated is not a sufficient reason to warrant discovery regarding every communication between the two agencies to fish for evidence that the United States had an impermissible role in the FLA's investigation.

In sum, defendant's Motion to Compel must be denied because defendant seeks to engage in a fishing expedition for evidence that would support defendant's speculative theories that the search warrant affidavit contains intentional misrepresentations material to a finding of probable cause. In the absence of a specific factual showing that the government possesses information helpful to defendant, defendant cannot satisfy Rule 16's materiality requirement.

Defendant's request for discovery pursuant to *Brady v. Maryland* also fails. The Due Process Clause requires the government to disclose "evidence favorable to an accused on request . . . where the evidence is material either to guilt or to punishment." *Brady v. Maryland*, 373 U.S. 83, 87 (1963). Importantly, "Rule 16 differs from *Brady*, which . . . provides the minimum amount of pretrial discovery granted in criminal cases." *Caro*, 597 F.3d at 620 (citing *United States v. Baker*, 453 F.3d 419, 424 (7th Cir. 2006)). For the reasons described above, defendant has not put forward non-conclusory arguments as to why the requested discovery would be helpful to the defense. Similarly, with respect to *Brady*, a narrower avenue of discovery than Rule 16, Fed. R. Crim. P., defendant's arguments fail to show that the government possesses any potentially favorable evidence that the government has not provided to defense counsel.

Defendant's request for discovery pursuant to the Sixth Amendment must also be denied. The Sixth Amendment guarantees criminal defendants the effective assistance of counsel.

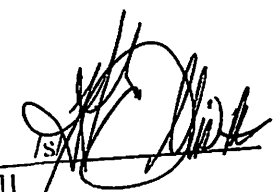
*Yarborough v. Gentry*, 540 U.S. 1, 5 (2003). Effective assistance of counsel is denied when “a defense attorney’s performance falls below an objective standard of reasonableness and thereby prejudices the defense.” *Id.* (citing *Wiggins v. Smith*, 539 U.S. 510, 521 (2003); *Strickland v. Washington*, 466 U.S. 668, 687 (1984)). Defendant has not presented any authority that supports the existence of a discovery obligation rooted in the Sixth Amendment. Thus, the Sixth Amendment does not provide an independent basis for obtaining discovery in this matter.

In summary, defendant is not entitled to additional discovery here because defendant has not satisfied the materiality requirement under Rule 16, Fed. R. Crim. P. Defendant has not provided facts—as opposed to mere speculation—that the government is in possession of information helpful to the defense. Nor has defendant shown that *Brady v. Maryland* or any other legal authority provides a basis for permitting additional discovery in this case.

An appropriate Order will issue separately.

The Clerk is directed to send a copy of this Sealed Memorandum Opinion to all counsel of record.

Alexandria, Virginia  
August 21, 2020



T. S. Ellis, III  
United States District Judge